# THE ECONOMIC FOUNDATIONS OF MILITARY POWER

Emily O. Goldman and Leo J. Blanken
University of California-Davis
2006-12

**About the Matthew B. Ridgway Center**

The Matthew B. Ridgway Center for International Security Studies at the University of Pittsburgh is dedicated to producing original and impartial analysis that informs policymakers who must confront diverse challenges to international and human security. Center programs address a range of security concerns – from the spread of terrorism and technologies of mass destruction to genocide, failed states, and the abuse of human rights in repressive regimes.

The Ridgway Center is affiliated with the Graduate School of Public and International Affairs (GSPIA) and the University Center for International Studies (UCIS), both at the University of Pittsburgh.

This working paper is one of several outcomes of the Ridgway Working Group on the Political Economy of International Security chaired by Peter Dombrowski, Sue Eckert and William Keller.

**The Economic Foundations of Military Power**

Emily O. Goldman, University of California, Davis
and
Leo J. Blanken, University of California, Davis

The fundamental premise of national security studies is the privileged position of the state as the key purveyor of violence. Commonly, the very form of the nation state is justified as the unit of political organization that achieves the most efficient economy of scale for generating violence (Bean 1973; Vries 2002, p. 144). Since the 1970s, advances in information, communication and transportation technologies, and the process of globalization they foster, have reduced the comparative advantages enjoyed by states in accumulating wealth and power, and monopolizing the means of destruction. Seen from this vantage point, the events of September 11 are one of the most vivid examples of the empowered non-state actor,[1] particularly because the events fall within the security domain. A non-state group inflicted a level of destruction normally associated with a state without donning the other encumbrances of that political organizational form. Predictions that terrorists might one day acquire weapons of mass destruction foreshadow even greater non-state empowerment.

Terrorism is not a new phenomenon, but it has assumed a more devastating scope. The attacks on the World Trade Center managed to kill an order of magnitude more Americans than Saddam Hussein achieved in two separate wars with one of the largest conventional armies in the world. The additional facts that non-state actors are relatively invulnerable to common tools of deterrence and defense, while the economic infrastructure that underwrites state power has become more vulnerable, have fueled claims that in the information age, technology is eclipsing the territorial state.

Have globalization and information technology altered the distribution of capabilities for violence, empowering non-state actors like terrorist and criminal organizations? Are the economies, societies and militaries of highly-networked, high-tech-dependent countries more vulnerable to disruption and destruction because their critical infrastructures are networked through computers? Does information technology favor organizational forms that hierarchical state bureaucracies find difficult to adopt?

It is premature to declare the information age has supplanted the industrial age, in the way that the age of agriculture passed into history with the emergence of new sources of energy, like steam and electricity, derived from fossil fuels. However, information has become a much larger part of the mix of resources– along with land, labor, and capital – for generating wealth and power. The questions are whether the links between economic power, the capacity to do harm,

and vulnerability, have been altered in important ways today in light of the informational underpinnings of advanced societies, and whether long standing relationships between economic capacity and military capability still hold. Are once-impotent adversaries being transformed into formidable foes?[2]

We argue non-state actors possess some distinct advantages over nation states, such as their invulnerability to common tools of coercion. Yet they sacrifice the ability to sustain an effective attack even against the soft and inviting targets of modern urban society. There is a difference between producing and sustaining destruction. The informational infrastructure of modern societies, economies and militaries produces vulnerabilities for states, yet the very infrastructure that makes states vulnerable is necessary in order for states to sustain modern military operations. Although changes in the relationship between economics and security in the information age have empowered non-state actors, states retain distinctive advantages because of, rather than in spite of, the economic infrastructure that supports their power.

To make our case, we compare the relationship between economic capability and military power in the industrial and information ages. We examine how the information age has affected warfare, and the conditions under which states retain their advantages in waging war. Because we are situated precisely at the transition between the industrial and information ages, the ability of organizations to adapt is critical. In this area states suffer some disadvantages, but these are not debilitating. We evaluate the factors affecting the military potential of states and non-states and conclude that lack of sustainability means non-state actors can only punish a state's vulnerable socio-economic targets, not erode its preeminence as the modal political unit in the foreseeable future.

**Economic Capability and Military Power in the Industrial Age**

Our understanding of the relationship between economic capability and military power was established in the context of a system dominated by state actors. Security studies approaches have been shaped by the sub-field's privileging of the externally sovereign Westphalian state and its counterpart the internally sovereign governmental state, as the most important unit of analysis. This partiality is grounded in historical reality: for 500 years states have reserved to themselves the right to carry out large scale public violence, and private actors rarely possessed significant military means (Spruyt 2002). Current leading approaches to the study of military power in the international relations sub-field remain grounded in the state.

Economic power does not translate directly into military power but the material basis of military strength has traditionally been a starting point for assessments of military potential, and economic capacity has been treated as a necessary condition for the ability to inflict significant

harm since the advent of the industrial age.[3] Paul Kennedy observed in 1987 the strong correlation between the productive and revenue-raising capacities of states and their military strength (1987, xvi).

Kennedy's remarks echo the neo-mercantilist proposition that economic capacity is a core foundation of military power[4] (Dorn 1963: 7; Heckscher 1936; Viner 1948). Large-scale modern warfare in the industrial age, best exemplified by the two world wars, illustrates the mercantilist position. Prevailing in lengthy wars of attrition depended not only upon the military forces a state could initially muster but also upon its ability to mobilize the underlying economic and industrial capacity of the state to produce combat power during war. War was not just a military conflagration but also a contest among entities that strive to understand and exploit the relationship between combat and economics.

The rise of the state itself as a form of political organization is largely viewed through the lens of war. Empires were too busy with coercion to provide a sound economic base, and city-states were too busy focusing on economic gain to provide adequate protection. Nation states carried the field by balancing the twin tasks of coercion and capital accumulation (Tilly 1990, pp. 22-29). States survive by waging wars, and wars are expensive. States generated revenue by taxing their subjects, or by borrowing. Whatever the sovereign's choice, robust economies are to be preferred to weak ones; a healthy economy is a source of power, and is therefore also a target (see Ripsman, this volume).

Tangible economic assets, like volume of GNP or size of defense industry, of course yield only a partial understanding of a state's military capacity. Intangibles, like a state's organizational ability and administrative competence to efficiently employ the resources at its disposal, are crucial, as are superior training and morale, which often compensate for inferior weaponry (van Crevald 1991, ch. 20). Countries also differ in their will to achieve military strength, and in the ability of leaders to impose costs on society (Milward 1977). Finally, the strategic environments of countries place different demands on armed forces (Geyer 1986). Even if a country possesses a comparatively small economy and weak technological base, these may still be sufficient for defending its territory from neighbors that are similarly equipped.

With the dawn of the nuclear age, the concept of economic "war potential" lost its relevance because modern weapons had made wars of attrition a thing of the past. The prospect of massive nuclear strikes and counterstrikes epitomized initial mobilization advantage and made all discussions of subsequent mobilization moot. Rather than discard the concept of war potential entirely, Klaus Knorr argued for adapting it to current conditions. The logic of mutual deterrence moved the locus of conflict below the nuclear level and as the Cold War superpowers embarked

on an arms race, the ability of the economy to sustain peacetime mobilization to support defense potential became critical. The concept of "defense potential" focused on a wider spectrum of defense efforts including the ability to sustain a peacetime military establishment and to recover from a nuclear attack. Only the most robust economy could develop and produce large numbers of complex weapons systems, while only the most prescient planners could at the same time address the vulnerability of the economic and social base.

If a shift from agricultural to industrial modes of production altered the foundations of military power, logically, the shift from the industrial to the post-industrial age should affect how international actors leverage different types of resources to increase their potential to inflict harm. By the end of the Cold War, for example, it appeared as if the Soviet Union had reached a high level of industrial maturity. In one key indicator of industrial capacity, steel production, the U.S.S.R. was producing 160 million tons per year in 1985, as compared to 74 million tons produced by the United States. Still, in the 1980s, even Soviet military strategists realized that their country could not keep pace with the West and they began writing about a military-technical revolution that they believed was underway in the West.

The information age is altering the economic foundations of modern advanced societies, while globalization has dramatically increased international flows of goods, services, people and money, improving access to information, technology, and their military applications. The information age presents new opportunities for states, but also new targets of vulnerability that can be exploited by empowered non-state actors.[5]

**Economic Capability and Military Power in the Information Age**

The relationship between wealth and power has changed as societies transition to the information age. Manuel Castells argues that technology does not determine society but "the ability or inability of societies to master technology, and particularly technologies that are strategically decisive in each historical period, largely shapes their destiny, to the point where we could say that while technology *per se* does not determine historical evolution and social change, technology (or the lack of it) embodies the capacity of societies to transform themselves…."(1996, p. 7).

Socio-economic change creates new military capabilities that can shift the relative influence of international actors (Organski 1958; 1968; Organski and Kugler 1980). Industrialization changed the pool of critical resources available to states, the capacity of states to utilize the human and material resources they possessed, and hence their capacity to wage war effectively (Organski and Kugler 1980, p. 9). Industrialization dramatically increased the level of productivity that could be extracted from any given population and hence the capacity of states to

generate wealth and wage war (Organski and Kugler 1980, pp. 8-9). Those states with a larger fraction of their total population of working and fighting age could realize more productivity from industrial technology, become more powerful, and wage war more effectively (Organski and Kugler 1980, p. 33). As industrial technologies and practices diffused to more and different states, those with the resources to exploit the new methods for economic productivity and military effectiveness gained international influence. Although there may be a lag time between socio-economic transition and how quickly militaries adapt, after the industrial revolution, the correlation between industrial and military power was very high.[6]

The information revolution suggests the process of improving resource utilization does not end with industrial maturity.[7] By fueling globalization, the information revolution enables states to increase productivity and enhance economic capacity by accessing new markets, expanding international trade, and increasing foreign direct investment (Castells 1996, p. 142) Email dramatically reduces the communications costs of doing business. The information revolution has also enabled some states to build remarkably advanced and lethal militaries that have produced extremely skewed results on the battlefield.

States have been resilient in the face of technological change, and despite the increasingly rapid diffusion of information, states still shape the political space within which information flows (Keohane and Nye 1998; Herrera 2004). Yet state power has been diminished too. States have lost much of their control over monetary and fiscal policies, which are often dictated by global markets (Castells 1996, pp. 245, 254). The rapid movement of currency in and out of countries by currency speculators can extract a devastating cost on countries that do not have large currency reserves. States no longer monopolize scientific research. The Internet allows a global scientific community to exchange information on topics that can be easily exploited by terrorist organizations (Castells 1996, p. 125). The Internet has made it impossible for states, dictatorships as well as democracies, to monopolize the truth (Castells 1996, pp. 384, 486-487). Nor can they monopolize strategic information (Keohane and Nye 1998) – the information that confers great advantage only if competitors do not possess it – because states no longer control encryption technologies.

Most critically, IT has made the most technologically advanced and powerful societies by traditional indices the most vulnerable to attack. A distinguishing hallmark of the information age is the "network," which exploits the accessibility and availability of information, and computational and communicative speed, to organize and disseminate knowledge cheaply and efficiently (Harknett 2003). The strength of the network lies in its degree of connectivity. Connectivity can increase prosperity and military effectiveness, but it also creates vulnerabilities.

Information-intensive military organizations are more vulnerable to information warfare because they are more information-dependent, while an adversary need not be information-dependent to disrupt the information lifeline of high-tech forces. Information-dependent societies are also more vulnerable to the infiltration of computer networks, databases, and the media, and to physical as well as cyber attacks on the very linkages upon which modern societies rely to function: communication, financial transaction, transportation, and energy resource networks. It would be foolish for a well-financed and motivated group not to attack the technical infrastructure of an adversary.

The same forces that have weakened states have empowered non-states. The information revolution has diffused and redistributed power to traditionally weaker actors. Terrorists have access to encryption technologies which increase their anonymity and make it difficult for states to disrupt and dismantle their operations. (Zanini and Edwards 2001, pp. 37-8) Global markets and the Internet make it possible to hire criminals, read about the design and dissemination of weapons of mass destruction, and coordinate international money laundering to finance nefarious activities (Kugler and Frost, eds. 2001; Castells 2000, pp. 172, 180-182). Terrorists can now communicate with wider audiences and with each other over greater distances, recruit new members, and diffuse and control their operations more widely and from afar. Non-state actors also have increasing access to offensive information warfare capabilities because of their relative cheapness, accessibility and commercial origins (US GAO 1996; Office of the Under Secretary for Defense for Acquisition and Technology 1996). Globalization, and the information technologies that undergird it, suggest that a small, well-organized group may be able to create the same havoc that was once the purview of states and large organizations with substantial amounts of resources.

Reliance on information technology also creates vulnerabilities for non-state actors. Computers centralize information, and confiscation of them by law enforcement agencies can undercut terrorist operations (Zanini and Edwards 2001, p. 40). Law enforcement and intelligence agencies are becoming increasingly adept at monitoring communications equipment – cell phones, satellite phones, and the Internet – for digital traces (Zanini and Edwards 2001, p. 39). Finally, the same global communications networks so adeptly exploited by terrorist and criminal groups can facilitate coordination among law enforcement and intelligence agencies worldwide to apprehend terrorists and gain valuable information about their future operations. Robert Keohane and Joseph Nye point out that the collection and production of intelligence information is very costly and states still retain significant advantages over non-states here (1998).

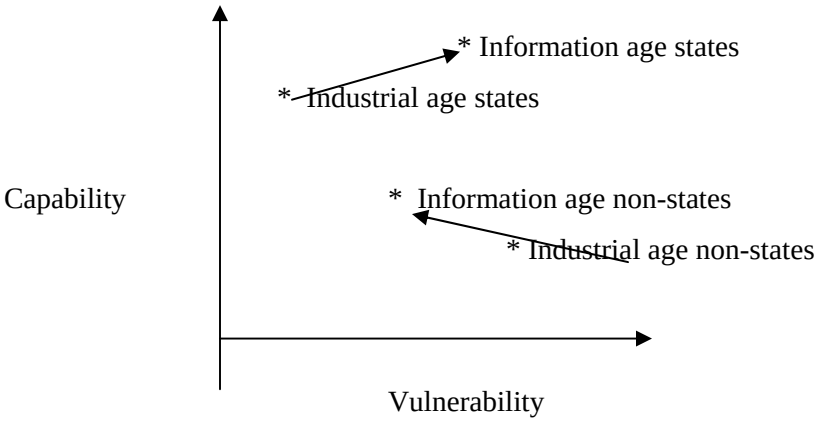
Table 1 summarizes the capabilities and vulnerabilities of states and non-state actors in the industrial and information ages. The difference between these two ages is that the industrial age skewed power toward states at the expense of non-state actors while the information age simultaneously advantages and disadvantages states and non-state actors.

**Table 1: Advantages and Disadvantages of States and Non-States**

| | Industrial Age | Information Age |
|---|---|---|
| States | ***Advantaged*** by centralized power and economies of scale for industrial production | ***Advantaged*** by ability to create and dominate information infrastructure<br><br>***Disadvantaged*** by susceptibility to disruption |
| Non-state actors (terrorists) | ***Disadvantaged*** by inability to generate wealth and power, or to exploit industrial production resources | ***Advantaged*** by decentralized power and ability to exploit information infrastructure<br><br>***Disadvantaged*** by inability to sustain attack |

The different capacities of states and non-states are also illustrated in Figure 1. Vulnerability is plotted along the x-axis and capability plotted along the y-axis. In the industrial age, states possessed high capability and low vulnerability to non-state actors, while non-state actors possessed the reverse -- high vulnerability to the coercive capacity of the state and low capability to threaten the state. In the information age, states have moved higher on the capability scale to the extent that they can leverage information technologies to generate greater violence. But they have also moved rightward, increasing their vulnerability precisely because they are more reliant on networks. Non-state actors have moved upward and toward the left, increasing their capabilities to inflict harm on states while decreasing their vulnerabilities to state coercion because information technologies afford them an unprecedented degree of coordination capability, global reach, and anonymity.

**Figure 1: Capability and Vulnerability in the Information Age**




**War and Destruction in the Information Age**

We have examined the impact of information technology on the capabilities and vulnerabilities of states and non-state actors. Now we focus on the consequences of these changes for waging war. The information age has increased the availability and affordability of information, information technologies, and information age weapons, and created new vulnerabilities for advanced information-dependent societies. The availability off-the-shelf commercial technologies benefits smaller states and non-state actors, to be sure, but only the wealthiest and most powerful states will be able to leverage information technology to launch a "revolution in military affairs." The ability to gather, sort, process, transfer, and disseminate information over a wide geographic area to produce dominant battle space awareness will be a capability reserved for the most powerful (Keohane and Nye 1998). In this respect, information technology continues trends already underway in the evolution of combat that have enhanced the military effectiveness of states. IT makes conventional combat more accurate, thereby improving the efficiency of high explosive attacks.

On the other hand, IT also continues trends in warfare that circumvent traditional military forces and which work in favor of weaker states and non-states. Like strategic bombing and counter-value nuclear targeting, efforts to destroy or punish an adversary by bypassing destruction of his armed forces and directly attacking his society, predate the information technology age. Techniques of information warfare provide attackers with a broader array of tools and an ability to target more precisely and by non-lethal means the lifelines upon which advanced societies rely: power grids, phone systems, transportation networks, and airplane guidance systems. Information is not only a means to boost the effectiveness of lethal technologies, but opens up the possibility of non-lethal attacks that can incapacitate, defeat, deter

or coerce an adversary, attacks that can be launched by individuals and private groups in addition to professional militaries. Warfare is no longer an activity exclusively the province of the state.

Some analysts remain skeptical that terrorists can overcome the technical and financial hurdles to inflict a highly damaging cyberattack (Soo Hoo, Goodman and Greenberg 1997; Thomas 2003; Weimann 2004). They argue terrorists are more likely to use IT for organizational rather than for offensive purposes (Zanini and Edwards 2001, pp. 46-50). Others point out that computer systems are remarkably resilient to attack, that sensitive military systems, the classified computers of intelligence agencies, and the Federal Aviation Administration's air traffic control system are physically isolated from the Internet (Lewis 2002). Yet private sector targets and critical infrastructure systems are far less secure, while the next generation of terrorists are growing up in a digital world and may see far more potential and have far more capacity for cyberterrorism (Weimann 2004). Globalization suggests it will be easier for the IT skills of the few to be leveraged by the many while studies of military diffusion show that a successful demonstration of a new form of warfare is a major impetus to its spread (Goldman and Eliason, eds. 2003).

The conceptual categories laid out in Table 2 clarify the relationships between information technology and warfare.[8] The state has a significant advantage only in Cells I and II.

**Table 2: Domains of Information Warfare**

| | **Target of attack** | |
|---|---|---|
| **Means of attack** | *Physical* | *Cyber* |
| *Physical* (hurling mass and/or energy) | ***I – Traditional War and Cyber-enhanced Physical Attack***<br><br>Bombing military or civilian facilities; conventional warfare or terrorism | ***II – Blast-based Information War***<br><br>Physical strikes on information infrastructure (e.g., 9-11 impacted cell phone switching area); EMP from directed-energy weapons that destroy or disrupt digital services |
| *Cyber* (hurling information) | ***III – Cyber-enabled Physical Attack***<br><br>Attacks on aircraft navigation system; spoofing air traffic control system; attacks on specialized digital devices that control electrical power and dam floodgates | ***IV – Non-lethal Information War***<br><br>Denial-of-service attacks, worms, logic bombs inserted into information systems, defacing web sites |

Cell I captures the characteristics of traditional warfare and cyber-enhanced physical attack. Information technologies augment conventional attack, as enablers of existing technologies by boosting the ability to find targets, direct fire to targets, as well as facilitating planning and communication among one's own forces. In several post-Cold War military engagements including the Persian Gulf War, Kosovo and Afghanistan, states used information technologies extremely effectively in battle to support and enhance traditional destructive warfare.

Cell II captures the idea that the information systems that undergird the operations of modern day societies and military organizations can be directly targeted through physical attack. Blast-based information war targets information systems with firepower. Physical attacks with conventional munitions on command and control targets, as well as on civilian critical infrastructure, such as electrical power generation and transmission systems, have been hallmarks of recent Western military campaigns. A new category of firepower – directed-energy weapons – uses high-power microwaves to disable electronic targets, in contrast to traditional jamming equipment that blocks communications devices from functioning but does not physically damage them. The new generation of directed-energy weapons "is meant to emulate the sort of damage that nuclear EMP [electro-magnetic pulse] can inflict upon electronics but at far less range, with more control of the damage and without all the ancillary physical destruction and radioactivity" (Schiesel 2003, pp. E1, E5).

Cell III, cyber-enabled physical attack, captures the destruction of physical targets by means of attacks on underlying technical systems. These attacks may be lethal, destroying lives and property, although only indirectly so. Recent attention has been directed toward the potential for terrorists to use the internet to target specialized digital devices, namely the distributed control systems (DCS) and supervisory control and data acquisition systems (SCADA) that throw railway switches and adjust valves in pipes that carry water, oil and gas. Increasingly, these digital control devices are connected to the Internet and lack rudimentary security. Moreover, utilities worldwide allow technicians to remotely manipulate digital controls, and information on how to do this is widely available (Gellman 2002, pp. 6-7).

Cell IV captures the pure form of information warfare—combat waged solely within the domain of information and information systems—which is non-lethal. The tools are "digital" and the targets include enemy population beliefs, enemy leadership beliefs, and the economic and political information systems upon which society relies to function.[9] The information age opens up the possibility of coercing and deterring adversaries, and influencing and shaping the strategic

environment in non-lethal ways. Cyber operations that target an adversary's digital systems or coordination capacity (military or societal) rather than their physical assets will disrupt, not destroy. Yet disruption can be combined with physical attack to produce destruction and defeat.

As states become more capable in executing cyber enhanced physical attack (Cell I) and blast-based information warfare (Cell II), with the United States dominating the global battlefield in conventional weapons, foreign governments and non-state actors are likely to resort to asymmetric strategies, like Cell III and Cell IV types of information warfare, terrorism, and weapons of mass destruction. These are ways of balancing the odds against a conventionally superior opponent. For weaker actors that cannot marshal the physical capability necessary to harm or influence more powerful adversaries, these methods of attack are likely to become strategies of choice. Particularly given an adversary with a highly informatized society and military, it makes logical sense to target the information systems of the adversary that provide intelligence about the opponents' tactics and strategy, that exercise command and control over, and direction of, capabilities and assets, and that undergird the functioning of the adversary's society and economy. It would be foolish to conclude that because there has not yet been a recorded instance of a major cyberattack, there will never be one. How many people were surprised by the events of 9/11?

**Adapting to Conflict in the Information Age**

More than in any previous era, the obstacles to acquiring leading edge technologies have fallen significantly. The physical limits on capabilities and resources that precluded states from modernizing their militaries in the past no longer exist. In the pre-industrial age, changes in the distribution of capabilities between and among nations took a long time. Efforts by one nation to increase its relative capabilities, either through territorial conquest or alliance formation, gave rise to a sufficiently even distribution of capabilities to prevent any one nation from subjugating others by means of war. This process was upset by the industrial revolution. The adoption of industrial technology provided nations with a far more rapid accretion in capabilities. Still, the roots of national power lay in natural resources and plant investment which were very costly.

Information power differs from industrial power in the speed with which it is likely to spread. Globalization accelerates this process. States unable to sustain a large modern defense industrial and technological base, as well as non-state actors, can rely on the international transfer of arms for access to advanced weapons systems. External sources of advanced technology have grown to include not only direct transfers of military technology from abroad, but purchases of advanced components and equipment from world commercial markets, and technology diffusion

from the state's civilian industries. Buying off the shelf allows states and non-state actors to obtain sophisticated equipment quickly.

But access to hardware is not enough. Organizations must be able to integrate and exploit the hardware, which requires specific human skill sets and the adaptation of organizational structures and processes.[10] During periods of rapid technological change, the ability to maintain or augment one's military power depends upon one's "transformational" potential, or how effectively one can absorb new technologies and implement accompanying practices. Indicators like defense expenditures or financial assets tell us little about transformational potential. Andrew Krepinevich compared French and German military expenditures during the interwar years and showed that France enjoyed a clear lead for nearly the entire period (Krepinevich 1994). Yet it was Germany that transformed its military to execute the *blitzkrieg* form of war and defeat France. In the same period, U.S. and Japanese Navy budgets were constrained, in the former case by the Great Depression and in the later case by bureaucratic subservience to the Japanese Army. Nevertheless, both transformed their battle-fleets and made the aircraft carrier the central offensive strike element. How much of a threat or challenge a particular modernizing military or terrorist group represents depends in large part on its capacity to assimilate new technologies and leverage new capabilities.

Success in the information age depends upon the ability to exploit information to a produce wealth and wage war,[11] and as in earlier periods, actors possess differing capacities. The size of a state's information industry is one indicator that it is developing into an information society and that its military is transitioning from an industrial to an informational one (Baocun 2001, p. 148). Taiwan's growing commercial high-tech sector and highly educated workforce has bolstered its military prowess in Asia (Bitzinger and Gill 1996, p. 36). Tiny Singapore's highly developed information technology and communications sector has allowed this country to modernize its military by exploiting IT (Huxley 2004; Singapore Ministry of Information and the Arts 2000, pp. 125-126).

Although a well-educated population that is familiar with information and communications technology facilitates absorption of technologically sophisticated systems by the military, wider societal familiarity with and receptivity to computers (Foster and Goodman 2000; Demchak 2000) is not a necessary condition for transformation. Roger Cliff, in his analysis of China's human capital base argues that "absolute numbers of scientists and engineers may be more important than numbers as a proportion of total population, and in this regard China compares more favorably with other countries" (Cliff 2001, p. xii). The important factor is

whether the society can sustain a high tech sector and whether scientists and engineers are effectively recruited from it into the military.

The ability to exploit information age technologies to wage war requires organizational adaptation. Richard Bitzinger and Bates Gill argue that the existence of a huge military-industrial complex, a large military R&D infrastructure and an expanding commercial high-tech base are not enough for China to be able to exploit the current RMA (Bitzinger and Gill 1996, p. 21). A variety of historical, organizational, managerial, technical and political factors present hindrances,[12] much in the way that although Taiwan possesses many technological and economic precursors to a deep RMA, political and bureaucratic constraints have impeded full exploitation of this potential capability (Mulvenon 2004). Organizational structures that facilitate the free-flow of information are better positioned to take advantage of current information-related military innovations. This explains the push in the U.S. military toward greater information sharing, more jointness, flatter command and control structures, reduced hierarchy, and more decentralized command and control.

Information is something that states, organized for success in the industrial age, do not have a comparative advantage in exploiting. John Arquilla and David Ronfeldt argue that the information revolution is strengthening the network form of organization over hierarchical forms, that non-state actors can organize into networks more easily than traditional hierarchical state actors, and that the master of the network will gain major advantages over hierarchies because hierarchies have a difficult time fighting networks. (Arquilla and Ronfeldt 2001, pp. 1, 15.)

States are run by large hierarchical organizations with clearly delineated structures and functions. By contrast, a more efficient organizational structure for the knowledge economy is the network of operatives, or "knowledge workers" not bound by geographic location. This is precisely the type of organizational structure being adopted by terrorist groups as they adapt to the information age.

There is evidence that adaptation is quicker in flat hierarchies or matrix organizations than it is in the steep pyramidal hierarchies that run the modern nation-state; that flatter networks have a much shorter learning curve than do hierarchically networked organizations (Areieli 2003). The higher the hierarchy, the faster it operates if it is doing something it has already foreseen and thus for which it is prepared. If, on the other hand, a scenario requires the development of new processes that were not foreseen, the flatter organization is better at learning. Matrix organizations are more creative and innovative.[13] According to Castells, the performance of a network depends on two fundamental attributes: "its *connectedness*, that is its structural ability to facilitate noise-free communication between its components; its *consistency*, that is the

extent to which there is sharing of interests between the network's goals and the goals of its components" (Castells 1996, p. 171). On both criteria, large state bureaucracies suffer serious disadvantages.

Table 3 summarizes the factors influencing the military potential of states and non-state actors today.

**Table 3: Military Potential of States and Non-States**

| **Factors affecting military potential** | **States** | **Non-state actors** |
|---|---|---|
| Economic capacity | Indigenous R&D; technology transfers | External linkages; consumer technology |
| Organizational constraints/obstacles | High; Steep hierarchical organizational structures with entrenched interests and bureaucratic rivalry innovate slowly | Low; Flat organizational structures more creative and adaptable |
| Knowledge paths | Social networks | Supplier networks; common training |
| Normative constraints | Taboos against certain practices | Few taboos |
| Globalization | Increases diffusion and levels playing field | Increases access and empowers |
| Vulnerability | High | Low |
| Ability to sustain military operations | High | Low |
| Ability to recover from attacks | ? | High |

Many of the debates on information warfare center on the resiliency, or recoverability, of states (center box, bottom row). It is simply not clear how susceptible to collapse the information infrastructure, society, and economic base of the United States are, if attacked in earnest. Many theorists argue that the integrated grids and networks are extraordinarily vulnerable to attacks at critical points, and that attacks will reverberate with special force through our fragile, liberal society (Molander et al. 1996; Lake 2000; Triplett 2000). Richard Betts calls this "the soft underbelly" of our primacy (2002; see also Byman and Waxman 1999). Specifically, Betts points out that in such situations the defender, despite overwhelming preponderance of military power, is asymmetrically eroded due to the inability to deter a non-state opponent, coupled with the enormous cost of defending itself everywhere at once. In short, if a major power is inordinately vulnerable in the information age, and if non-state actors can wage a sustained campaign, then we might conclude that the future looks grim for the major powers of the world.

The truth is we simply do not know the extent to which the information age has altered the recoverability of advanced, wealthy economies. The Y2K scare played on the fear of the delicacy and interconnectedness of information systems, and yet failed to produce any noticeable effects. Major and extended blackouts in the Northeast and Midwest of the United States and Canada in the summer of 2003 (which would have been a major coup if accomplished by a terrorist group) failed to produce the mayhem, crime, and social dislocation of lesser blackouts in the 1970s. The dynamics of such a complex system as the United States, or a similarly advanced state, precludes a clear answer.

The other boxes worth noting are the first and third down in the right-hand column, which list the economic capacity and knowledge paths of terrorist groups. States are frequently in the business of generating large-scale violence; to generate violence, however, weapons are needed. States are then confronted with the classic economic problem of 'make or buy'.[14] Non-state actors usually are forced to rely on the 'buy' option. They gather whatever conventional weapons available, through whatever means possible, and apply them as best they can.[15]

How does the information age alter this scenario? Besides monetary support from external sources, 'consumer technology' is a source of economic capacity. This is best described by Betts, who writes:

> Nineteen men from technologically backward societies did not have to rely on home-grown instruments...They used computers and modern financial procedures with facility, and they forcibly appropriated the aviation technology of the West and used it as a weapon (2002, p.25; see also van Creveld 1991, p. 306).

In the liberal, informatized world weapons are everywhere if one is able to see the correct combination of consumer technologies. Though information technology has been diffused to and exploited by non-state actors in the past (such as the printing press) it has never been used to generate large scale violence. This is a significant break with the past.

**Attacking the Base: Sustainability and Vulnerability**

The transition from the industrial to the information era has undercut many of the strengths we have traditionally associated with great power status. For non-state actors, the information age presents new opportunities that in some cases do not carry with them attendant vulnerabilities. Non-state actors can employ information technology to project destructive power without having to maintain a large industrial or information infrastructure that itself would present a target. Yet just how susceptible are states to force directed at their social and economic base?

The answer depends on the nature of the trade-off between power and vulnerability. In other words, the greater the industrial base which provides the material of modern war, the greater the dependence a state has on the fixed and relatively soft targets of modern society (industry and its supporting infrastructure). These targets have been discussed in an operational context (most extensively in the strategic bombing literature), but there has been little effort to link this to the set of broader questions implied above: What advantages accrue to the nation state and its relatively vast potential for sustained war making (versus non-state actors)? What disadvantages accrue to the nation state in terms of the access to and vulnerability of its economic base during war? Conversely, what advantages and disadvantages do non-state actors possess or lack in these areas? Additionally, how do these relationships change in light of the transition from the industrial age to the information age?

First we must discuss the relationship between sustained military force and the economic foundations of power. In the industrial age, a positive relationship has commonly been assumed to exist between the ability to sustain military force and the vulnerability of the societal base. This is evident from a brief examination of the evolution of industrial-age operational theory regarding the targeting of the economic base of an enemy. The literature, however, frequently conflates two components of an enemy's war making capabilities: economic base and the society's will to resist. As will be shown below, punishment aimed at eroding a society's will to resist is rarely successful. Attacking the state's economic base is a viable means of disabling an opponent, but this is only possible after delivering an enormous amount of punishment. As a result, although non-state actors can remain largely invulnerable to a nation state's tools of deterrence and defense, this invulnerability is purchased at the cost of sustainability. Without the ability to mount a sustained attack they will have a difficult time producing significant effects on the economies of modern states.[16]

The American civil war is sometimes argued to be the first "modern" war -- modern in the sense that victory was decided not just by the size, skill, and leadership of the opposing military forces, but also by the burgeoning industrial capabilities of both sides. Not only was this component part of the offensive capabilities of each side, it also became a target. William T. Sherman realized that industrial age wars could not be won by solely concentrating on the decisive battlefield engagements of the Napoleonic tradition, but required methodical dismantling of the opponent's economic base. Civil War historian James McPherson has argued that Sherman's campaign prefigured the strategic bombing campaigns of World War II. Sherman "preferred to destroy wealth and property that sustained the enemy army rather than that army itself" (quoted in Castel 2003: 421).

French naval policy in the post-Crimean War period also shows a burgeoning appreciation of strangling an opponent's economic base. The French *Jeune Ecole* hoped to embrace the naval technological revolution of the mid-nineteenth century to offset the much larger and more powerful British navy. Their program of commerce raiding and coastal barrage recognized the British weakness for supplying its population and industries with foodstuffs and raw materials from abroad. Instead of losing the race of battleship procurement, it was wiser to invest in cheaper, faster ships, which could cut Britain's economic base off at the knees (Marder 1940). Once again, the focus was on circumnavigating the tough defensive shell of the opponent, and seeking the soft and vulnerable links in the economic chain.

This thread of strategic thought came into its own with the advent of air power. Early theorists such as Guido Douhet and Billy Mitchell developed operational doctrines that maximized the disjuncture between battlefield success and the erosion of economic capability to sustain a war effort. In a world reeling from the bloody stalemates of the Western front, planners of the inter-war period had high hopes for bringing a more decisive instrument of coercion to bear in future conflicts (Biddle 2001). The logic behind strategic air power flowed directly from Sherman's campaign in Georgia and the French *Jeune Ecole*: evade the enemy's military forces, seek out and cripple the economic base which is a necessary component for war making in the industrial age. World War II provided the first and best example of these types of air campaigns, and the punishment of vulnerable targets culminated in Hiroshima, which laid the basis for nuclear deterrence in the Cold War (Quester 1966).

One key problem with these theories is their tendency to conflate two theoretically distinct but empirically intertwined variables: physical economic capabilities and the will to resist (Pape 1996: 57). Targeting civilian areas serves the dual purpose of inhibiting the state from replenishing material losses on the battlefield, and inciting the population to cry out for an end to the punishment.[17] It erodes both the physical and psychological capability of the enemy to resist. It is rarely made clear which is more effective, or if one aim can be achieved without the other. Operationally, the question is often moot. As Hugh Trenchard argued to the British Cabinet in 1941:

> If you are bombing at sea, then 99 percent of your bombs are wasted, but not only 99 percent of the bombs are wasted but 99 percent too, of the pilots and of the training which went to produce them…If, however, our bombs are dropped in Germany then 99 percent which will miss the military targets all help to kill, damage, frighten, or interfere with Germans in Germany, and the whole 100 percent of the bomber organization is doing useful work and not merely 1 percent of it (Murray 1992: 245).

This practical arithmetic suggests that targeting physical economic facilities could produce the desirable externalities of punishing the will to resist of the German people. In the age of largely imprecise (dumb) bombing, it was unimportant which factor had a larger independent effect since both were being inflicted by the same operational policy.

The most recent and refined progeny of this doctrine is known as "effects-based" operations (or EBO). Targets are chosen to produce indirect as well direct effects; these second- and third-order effects are designed to produce non-linear shockwaves that reverberate through the target society and directly erode the enemy's will and ability to fight (Beagle 2001; Cordesman and Arleigh 2003). It is hoped that "rather than relying on old approaches of annihilation or attrition, this new way of conducting operations will focus on generating desired effects [as opposed to] objectives or the physical destruction of targets" (Batschelet 2002, p. 2). It is implied in this doctrine that the more complex, interdependent, and concentrated a society is, the more susceptible it is to such attacks.

Recent empirical research has shown, however, that punishment strategies (such as those of Douhet, Schelling, and some "effects-based" planners) rarely work in military conflicts (Pape 1996; 1997/98). William Arkin found in the air war over Kosovo that NATO bombing actually solidified the will of the Serbian populace; only after an extended, intense, and technologically unprecedented strategic bombing campaign did pressure come to bear on Milosevic (Arkin 2001). T.W. Beagle agrees. After examining four American bombing campaigns (one each from the Second World War, the Vietnam War, the Gulf War, and Kosovo) he concedes that the air force has been good at generating tactical effects, but less so at the operational or strategic level and concludes that "the most sought-after effects are often psychological in nature, and efforts to improve airpower's capabilities in this area are virtually non-existent" (Beagle 2001, p.3).

Rather than as a psychological weapon air power seems better employed in wartime as a tool of degrading the military capabilities of the opponent on, or immediately behind, the front lines. Airpower, despite the claims of proponents, appears to only degrade the economy of a state through a sustained and massive application.[18] This is important for the discussion at hand. If non-state actors use terrorist attacks against the vulnerable homeland of nation states, is the target the physical (economic capabilities of the nation state), or the psychological (the will of the populace to resist the terrorists' demands)? If it is the former, such attacks are only likely to succeed if they can be sustained and significant.[19] If it is the latter, they may just serve to stiffen the resolve of the opponent.[20] As a result, they are unlikely to be successful in achieving their aims, if these aims include bending powerful nation states to their will. They may be able to change some aspect of policy, disrupt some aspect of economic or social normalcy, or gain some

other minor concessions.[21] They will not be able to 'defeat' a 'normal' state, in the military sense because they do not have the societal, industrial, and financial base to apply a significant amount of force consistently.

**Conclusion**

Despite more capable non-state actors and increasing state vulnerabilities, the nation-state retains the optimal economy of scale for generating wealth and violence. The important issues are how states and non-states have been both empowered and weakened, and how adaptable they are to the exigencies of conflict in the future.

Terrorist groups have proved to be adaptable and flexible, difficult to deter and defeat. Yet the very structures that terrorist groups use to their advantage against deterrence and defense robs them of the ability to sustain their energy on the 'battlefield', even of that battlefield is the opponent's domestic landscape. If they attained the infrastructure and assets required to seriously undermine an advanced economy such as that of the United States, they would sacrifice the veil of anonymity, which is their greatest advantage. Yet without sustainability, these actors must fall back on a punishment strategy, which is more likely to galvanize the opponent than it is to achieve its goals.[22]

---

[1] We are concerned with those non-state actors bent on waging war and violence in the international system. Hence, we do not focus on the full range of non-state actors, including multinational corporations, non-governmental organizations and inter-governmental organizations.

[2] This is the question posed by David S. Alberts, John J. Garstka, and Frederick P. Stein in *Network Centric Warfare* (September 1999).

[3] This is evident from a perusal of the literature stemming back to List and Hamilton (Earle 1986), up to Kennedy (Kennedy 1987) and Friedberg (Friedberg 1988), and through the Cold War (Kapstein 1992: xiii). For all these theorists, a sizable economic base was a necessary condition for military power. The question was, given a decent economic base, how did the state manipulate its economic potential to extract the maximum amount of military power (or overall national security) from it?

[4] This is the notion of neo-mercantilism versus traditional mercantilism because it accepts the fact that military power is predicated on the strength of the economy, rather than stored bullion. For a discussion see Goodwin (1991, pp 27-29).

[5] The impact of improved information technology on the military has, of course, been noted and studied prior to the advent of the information age. For example, see Dennis Showalter's analysis of the impact of the electric telegraph on Prussia's command structure (1973).

[6] This was because of the tremendous capital investment required to produce a modern mass production industrial base for warfare in the industrial age. The correlation need not be so close in the information age.

[7] This is the thesis the Tofflers adopt when they explain their three civilizations and war forms: agricultural, industrial, and information. See Alvin and Heidi Toffler, *War and Anti-War* (New York: Warner, 1993). For a critique of the Tofflers, see Robert J. Bunker, "The Tofflerian Paradox," *Military Review* (May-June 1995), pp. 99-102.

[8] This table is adapted from Bishop and Goldman 2003.
[9] In this respect, non-lethal information warfare also includes perception management and propaganda. See Zanini and Edwards 2001, pp. 41-44.
[10] See Douglas A. Macgregor, *Transformation Under Fire: Revolutionizing How America Fights* (Westport, CT: Praeger, 2003) for a discussion of how the U.S. military must transform its organizational structure to exploit new technologies.
[11] For a more comprehensive analysis of the political, economic, social, cultural and organizational factors shaping the ability of states to assimilate and master the use of advanced information technologies in the military sector, see Emily O. Goldman, "Military Diffusion and Transformation," in Emily O. Goldman and Thomas G. Mahnken, eds., *The Revolution in Military Affairs in Asia* (Palgrave, 2004 forthcoming).

[12] China suffers from low interconnectedness, high formalism, and low organizational slack. China's military and commercial sectors are segregated, which inhibits cross-fertilization and diffusion of commercial technologies and organizational principles to the defense sector and the ability of the military to benefit from spin-on of locally available commercial technology. Bureaucratic formalism pervades organizational norms such that meeting production quotas is valued over innovation. Central planning reduces organizational slack and surplus capacity for producers to innovate outside the "plan." Finally, incentives in the production of dual use technologies are for lucrative commercial applications and markets, not spin-on efforts to support military modernization.
[13] I am indebted to Chris Demchak for bringing these distinctions to my attention.
[14] It may serve a state's short-term interest to buy off-the-shelf systems from an ally. This may not be the best long-term solution however, as the purchaser becomes dependent on the flow of technicians and spare parts. For example, China's aeronautics industries (both military and commercial) have been significantly retarded by its reliance on Soviet equipment (Allen 2000).
[15] Under certain specified conditions non-state actors can challenge states on the field of battle, even in the industrial age. For discussions see Taw and Hoffman (1994) and Arreguin-Toft (2001).
[16] A single incident of maritime terrorism which could close down one or more hub ports critical to world trade could have a devastating impact on the global economy. For example, it has been estimated that the global economic impact from a closure of the port of Singapore alone could exceed US$200b per year from disruptions to inventory and production cycles. Shutting down of ports on the west coast of the United States could cost up to US$1b a day. (Ho 2004)
[17] For example, in the strategic bombing campaign of Japan during the Second World War, US planners had the "strong opinion, that the will of the Japanese people and of its government to resist could be greatly weakened and perhaps destroyed by urban area [incendiary] attacks" (United States Strategic Bombing Survey 1946, p. 37).
[18] For example, Germany maintained a viable economy during the Second World War until December of 1944 despite roughly 1.8 million tons of bombs having been dropped on it by that point (United States Bombing Survey 1945, p. 2; see also the extended discussion in Milward 1965).
[19] Osama bin Laden, in discussing the September 11 attacks, argued hopefully for a sustained campaign against the economic base of United States: "These blessed strikes showed clearly that this arrogant power, America, rests on a powerful but precarious economy, which rapidly crumbled...the global economy based on usury, which America uses along with its military might to impose infidelity and humiliation on oppressed people, can easily crumble...Hit the economy, which is the basis of military might. If their economy is finished, they will become too busy to enslave oppressed people. ... America is in decline; the economic drain is continuing but more

strikes are required and the youths must strike the key sectors of the American economy" (quoted in Betts 2002, p. 25 ff 11).

[20] Betts argues that terrorist groups may underestimate American resolve, and that when vital interests are at stake "primacy unleashed may prove fearsomely potent" (2002, p.35).

[21] For an analysis of suicide bombing in particular see Pape (2003).

[22] The attacks of September 11 did serve to galvanize American support for extensive overseas interventions. In a very crude calculus, the terrorists toppled two buildings, and in response, the United States toppled two regimes (those of Afghanistan and Iraq).